

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Content of the Kik account associated with  
username Grace.\_law, including content of communications,  
that is stored at premises controlled by MediaLab, Inc.

Case No.

2:21-mj-3917

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 USC Secs 2252 and 2252A Receipt/possession/accessing with intent to view of child pornography/visual depictions of minors engaged in sexually explicit conduct in interstate commerce

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew McCabe, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 9/16/2021City and state: Columbus, Ohio  
Elizabeth A. Preston Deavers  
United States Magistrate Judge

Elizabeth A. Preston Deavers, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
EASTERN DIVISION

In the Matter of the Search of:

Content of the Kik account associated with the  
Username Grace.\_law, including content of  
communications, that is stored at the premises  
controlled by MediaLab, Inc. located at  
1237 7<sup>th</sup> Street, Santa Monica, CA 90401

)  
)  
)  
)  
)  
)  
)

No.

Magistrate Judge

UNDER SEAL

**APPLICATION FOR ORDER COMMANDING KIK NOT TO NOTIFY ANY PERSON  
OF THE EXISTENCE OF LEGAL PROCESS  
PURSUANT TO 18 U.S.C. § 2705(b)**

The United States requests that the Court order the Electronic Service Provider Kik via MediaLab, Inc. not to notify the person (including the subscribers or customers of the account(s)) listed in the attached legal process, which requests a search warrant for subscriber information and content of communications for the user name Grace.\_law, including name, address, instrument used, length of service and IP address log-in information, of the existence of the legal process until further order of the Court.

Kik via MediaLab, Inc. is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 3486, the United States issued a search warrant, which requires Kik via MediaLab, Inc. to disclose certain records and information to the United States.

This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.*

In this case, such an order would be appropriate because the attached search warrant relates to an ongoing criminal investigation involving child exploitation that is neither public nor known to the targets of the investigation, and its disclosure may alert the target to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation, including by giving the target an opportunity to flee or destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Some of the evidence in this investigation is stored electronically. If alerted to the investigation, the subject under investigation could destroy that evidence, including information saved to their personal computers.

WHEREFORE, the United States respectfully requests that the Court grant the attached Order directing Kik via MediaLab, Inc. not to disclose the existence or content of the attached search warrant, except Kik via MediaLab, Inc. may disclose the attached legal process to an attorney, for Kik via MediaLab, Inc. for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court; and that three (3) certified copies of the Order and this Application be provided by the Clerk of the Court to the United States Attorney's Office. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to of the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Executed on September 13, 2021.

Respectfully submitted,

VIPAL J. PATEL

Acting United States Attorney

/s/ Emily Czerniejewski

EMILY CZERNIEJEWSKI (IL 6308829)

Assistant United States Attorney

303 Marconi Boulevard, Suite 200

Columbus, Ohio 43215

Office: (614) 406-3572

Fax: (614) 469-5653

E-mail: [emily.czerniejewski@usdoj.gov](mailto:emily.czerniejewski@usdoj.gov)



**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
EASTERN DIVISION**

<b>In the Matter of the Search of:</b>	)	<b>No.</b>
	)	
<b>Content of the Kik account associated with the Username Grace._law, including content of communications, that is stored at the premises controlled by MediaLab, Inc. located at 1237 7<sup>th</sup> Street, Santa Monica, CA 90401</b>	) ) ) ) ) )	<b>Magistrate Judge</b>
	)	<b><u>UNDER SEAL</u></b>

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Andrew D. McCabe, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

**I. EDUCATION TRAINING AND EXPERIENCE**

1. I am a Special Agent with the FBI assigned to the Cincinnati Division, Cambridge Resident Agency and I have been a Special Agent since September 2010. I am currently assigned to Cambridge Resident Agency and I am a member of the Child Exploitation and Human Trafficking Task Force. During my tenure as an FBI Special Agent, I have investigated numerous crimes including, but not limited to, bank robbery, drug trafficking, racketeering, kidnaping, violent extremism, and crimes against children.

2. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Special Agent, I investigate violent crime against children in violation of 18 U.S.C. §§ 2251, *et seq* and 2421, *et seq*.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

**II. PURPOSE OF THE AFFIDAVIT**

4. I make this affidavit in support of an application for a search warrant for information associated with a certain Kik user account/ID that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., a social networking company headquartered in Santa Monica, California. This affidavit is made in support of an application

for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab, Inc. to disclose to the government records and other information in its possession (including the content of communications), pertaining to the subscriber or customer associated with the **Kik username Grace.\_law (the SUBJECT ACCOUNT)**, which is stored at the premises owned, maintained, controlled, or operated by MediaLab, Inc. located at 1237 7<sup>th</sup> St., Santa Monica, CA 90401. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

5. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of the **SUBJECT ACCOUNT**. I have not omitted any facts that would negate probable cause.

6. The **SUBJECT ACCOUNT** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252 and 2252(a) – distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entire content of the **SUBJECT ACCOUNT**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

### **III. APPLICABLE STATUTES AND DEFINITIONS**

7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

8. Title 18, United States Code, Section 2252A, makes it a federal crime for any

person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

9. As it used in 18 U.S.C. §§ 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

10. As it is used in 18 U.S.C. § 2252A, the term “child pornography”<sup>1</sup> is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

11. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”

12. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.”

13. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C.

---

<sup>1</sup> The term child pornography is used throughout this affidavit. All references to this term in this affidavit, and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).



§ 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.

14. The term “computer”<sup>2</sup> is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

#### **IV. BACKGROUND REGARDING THE INTERNET, MOBILE APPLICATIONS AND KIK MESSENGER**

15. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and conversations with other officers, I know the following:

16. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol addresses and other information both in computer data format and in written record format.

17. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device. Storing this

---

<sup>2</sup> The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.



information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

18. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, Kik messenger service, Snapchat, Meet24, and Twitter.

19. From my review of publicly available information provided by Kik Messenger administrators I am aware of the following about Kik Messenger and about the information collected and retained by Kik Messenger.

20. Kik Messenger owns and operates a free-access mobile device messenger service that lets users connect with other users through chat. Kik Messenger allows users to create a profile from which they can send text, pictures, videos and more to other users from around the world. Users can only access Kik Messenger using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

21. Upon registration, Kik Messenger users create unique usernames which cannot be replicated and an account password. Kik Messenger also asks users to provide first and last name, date of birth and email address upon registration. Users are also able to create a profile picture and a background picture. This information is collected and maintained by Kik messenger.

22. Kik Messenger collects and maintains information on the particular devices used to access the application. In particular, Kik Messenger may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access KIK Messenger.

23. For each user, KIK Messenger also collects and retains the following information:

- a. Transactional Chat Logs, a log of all the messages that a user has sent and received, including sender username, receiver username/receiver group JID, timestamps, IP of the sender and word count. This log does not include the actual message that was sent. If the message was received by the subject user in a group, the log will contain the receiver group JID, not all receiver usernames;
- b. Chat Platform Log, a log all the media files that a user has sent and received, including sender username, receiver username/receiver group JID, timestamps, IP of the sender, media type, and Content ID. If the message was received by the subject user in a group, the log will contain the receiver group JID, not all receiver usernames;
- c. Photographs and/or videos o Media files sent or received by the user for the last 30 days;
- d. Roster log of usernames added and blocked by the subject user, including timestamps;
- e. Abuse reports;
- f. Transcript of reported chat history against the subject user, including sender username, receiver username, timestamps, actual message, and content IDs;
- g. Log of all the emails that have been associated with a username;
- h. IP address associated to the username when the account was registered, including timestamp.
- i. Email events;
- j. Registration IP

24. As explained herein, information stored in connection with a Kik Messenger account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Kik Messenger user’s account activity, IP log, stored electronic communications, and other data retained by Kik Messenger, can indicate who has used or controlled the Kik account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-

location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Kik Messenger account activity can show how and when the account was accessed or used. For example, as described herein, Kik Messenger logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Kik Messenger access, use, and events relating to the crime under investigation. Last, KIK Messenger account activity may provide relevant insight into the KIK Messenger account owner's state of mind as it relates to the offense under investigation.

25. Based on the information above, the computers of KIK Messenger are likely to contain all the material described above with respect to the **SUBJECT ACCOUNT**, including stored photographs, videos and information concerning subscribers and their use of Kik Messenger, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

#### **V. INVESTIGATION AND PROBABLE CAUSE**

26. On or about July 26, 2019, law enforcement officers in Putnam County, New York initiated an investigation into the online sexual exploitation of 14-year-old Minor Victim. Through their investigation, law enforcement identified an individual who both requested and received child sexual abuse materials from Minor Victim via the Kik mobile application. Specifically, that individual communicated with Minor Victim while utilizing the Kik username jimmy.merry04. Law enforcement in New York were able to ascertain that the Kik account associated with the username jimmy.merry04 was registered to James MERRY with a possible address in Muskingum County, OH. The communications between Kik username jimmy.merry04 and the Minor Victim's Kik account began on or about June 27, 2019 and continued until on or about November 24, 2019.

27. On or about January 20, 2020, the Federal Bureau of Investigation (FBI) opened an investigation into the exploitation of Minor Victim by MERRY. In October 2020, the case was then referred to the Muskingum County Sheriff's Office (MCSO) in Zainesville, Ohio and



your affiant after it was confirmed that MERRY resided in Ohio within your affiant's jurisdiction. Your affiant then conducted a joint investigation with law enforcement from the MCSO.

28. On or about March 11, 2021, an administrative subpoena was served on Kik requesting subscriber information for Kik username jimmy.merry04. On March 19, 2021, Kik responded to that subpoena with the following information:

Email Address: jimmy.merry23@yahoo.com

Registration Date: December 23, 2014

29. In addition, Kik provided a list of IP addresses that were used to access the Kik account for jimmy.merry04. A subsequent review of the IP address log provided indicated that the following IP addresses were used to access the jimmy.merry04 Kik account at or about the same times the Minor Victim was in contact with the jimmy.merry04 Kik account:

1. 71.72.69.91;
2. 174.233.163.222;
3. 174.233.147.52;
4. 174.233.155.204;
5. 174.233.143.21;
6. 174.233.142.115;
7. 174.233.7.238;
8. 174.233.138.13;
9. 174.233.134.187;
10. 107.11.90.86;
11. 107.11.69.249;

30. Further investigation revealed that eight of the eleven IP addresses from the above noted list were resolved to Verizon Wireless:

1. 174.233.163.222
2. 174.233.147.52
3. 174.233.155.204
4. 174.233.143.21
5. 174.233.142.115
6. 174.233.7.238



7. 174.233.138.13

8. 174.233.134.187

31. Your affiant then learned that the last three IP addresses provided by Kik were resolved to Charter Communication, specifically, the IP address 71.72.69.91, 107.11.90.86, and 107.11.69.249.

32. On May 18, 2021, an administrative subpoena was served on Charter Communications requesting subscriber information for the IP addresses 71.72.69.91, 107.11.90.86, and 107.11.69.249. On May 21, 2021, Charter Communication responded with the following information regarding IP address 71.72.69.91:

Name: James Merry

Service/Billing Address: 91 N Pembroke Avenue, Zanesville, Ohio 43701

Billing Email: jmerry71@gmail.com

Telephone Number: (740) 453-0633

Charter Communication additionally provided the following information regarding IP addresses 107.11.90.86 and 107.11.69.249:

Name: Douglas Merry

Service/Billing Address: 93731 Ridgeland Dr. Nashport, Ohio 43830

Billing Email: niteowlcop@gmail.com

Telephone Number: (740) 453-0633

33. Your affiant then learned through his investigation that Douglas Merry is the father of James MERRY, the target of the investigation related to Minor Victim.

34. On May 18, 2021, an administrative subpoena was served on Verizon Wireless requesting subscriber information related to the eight IP addresses noted in the Kik subpoena return subscribed to Verizon. On May 19, 2021, in response to an administrative subpoena, Verizon Wireless informed the FBI they only stored IP address records for 365 days. As such they were unable to comply with the subpoena since the information was no longer retained in their database.

35. Based on the registration email listed in the Kik responses, an administrative subpoena was sent to Oath Holdings on April 22, 2021, for subscriber information pertaining to the Yahoo email account jimmy.merry23@yahoo.com. On or about April 28, 2021, in response to an administrative subpoena, Oath Holdings provided the following information:

Name: Jimmy Merry

Subscriber Phone Number: (740) 624-9575

36. Your affiant noted that the telephone number (740) 624-9575 was serviced by Verizon Wireless and an administrative subpoena was then sent to Verizon Wireless to ascertain subscriber information associated with that telephone number. On or about May 13, 2021, in response to the administrative subpoena, Verizon Wireless provided the following information:

Subscriber Name: Douglas Merry

Service/Billing Address: 93731 Ridgeland Dr. Nashport, OH 43830

Identified User: James Merry

Phone Identifiers: Motorola Moto Z2.

37. On or about June 15, 2021, an interview was attempted with James MERRY at the address of 93731 Ridgeland Drive in Nashport, Ohio. Your affiant learned that MERRY was not at the residence but was currently employed at a McDonalds located on the south side of Zanesville, Ohio.

38. On or about June 15, 2021, an interview with MERRY took place at the McDonalds MERRY was employed at. More specifically, MERRY was interviewed in your affiant's FBI vehicle in the McDonalds parking lot. MERRY was advised that his participation in the interview was voluntary and he could leave at any time.

39. During the interview, MERRY admitted to requesting sexually explicit images from Minor Victim as well as other minor children on various social media platforms. MERRY identified Twitter and Kik as social media applications he utilized to make these requests for child exploitation material. MERRY also admitted to currently possessing sexually explicit images of minor children on his cellular phone, a black Motorola Moto Z2.

40. MERRY signed a written consent for a search of his black Motorola Moto Z2 and provided the cell phone to law enforcement. Your affiant conducted an on-scene review of MERRY's Motorola Moto Z2 and observed what appeared to be sexually explicit images of children. When confronted with this information, MERRY voluntarily surrendered his cellular phone to law enforcement and verbally consented to a forensic examination of his cellular telephone.

41. On or about June 17, 2021, MERRY was arrested by the Muskingum County Sheriff's Office (MCSO) and charged with twelve counts of pandering obscenity involving a

minor. On or about August 9, 2021, MERRY plead guilty to those charges and his sentencing hearing is pending.

42. In assisting the MCSO with their investigation of MERRY, the Federal Bureau of Investigations (FBI) took custody of the black Motorola Moto Z2 belonging to MERRY. On July 21, 2021, the FBI completed a forensic analysis of MERRY's black Motorola Moto Z2 cellular telephone.

43. On or about June 22, 2021, the results from the forensic extraction of MERRY's cellular phone were reviewed. Your affiant noted MERRY was in possession of over 75 sexually explicit images of children. In general, these images depicted prepubescent females engaged in the lascivious display of genitalia, masturbation, and sex acts with adults. Specifically, the following sample of child exploitation images were recovered from MERRY's black Motorola Moto Z2:

1. One image depicting a naked prepubescent female, white reclining on a blue sheet with her arms behind her head. The female's legs are bent and spread in such a way as to display her nude genitalia.
2. One image depicting a prepubescent female wearing a pink shirt reclining on a bed with her arms wrapped under her legs, spreading them in such a way as to display her nude genitalia.
3. One image depicting a prepubescent female, white with blond hair wearing a grey t-shirt inserting her fingers into her vagina.
4. One image depicting a prepubescent female wearing a white shirt engaged in vaginal sex with a male white of undetermined age.
5. One image depicting a prepubescent female bent over displaying her nude genitalia and anus. The minor female is observed to be inserting her fingers into her anus.
6. One image depicting a prepubescent female wearing a pink shirt kneeling on a bed performing oral sex on the penis of an adult male.
7. One image depicting a prepubescent female wearing pink and white striped underwear engaged in vaginal sex with a male of undetermined age.

44. In reviewing the forensic extraction of MERRY's Motorola Moto Z2, your affiant noted that no Kik Messenger content was captured during the forensic examination despite the fact that the Kik Messenger application was installed on MERRY's cellular phone.

45. On or about June 23, 2021, your affiant conducted a manual review of the Kik



Messenger application that was installed on MERRY's Motorola Moto Z2 cellular phone. Your affiant observed that the Kik Messenger application on MERRY's phone had a username of john.drew87 logged in.

46. During the manual review of the john.drew87 account, your affiant noted the following exchange of messages occurring between john.drew87 and another Kik user with the username Grace.\_law, **SUBJECT ACCOUNT**. The exchange of messages between john.drew87 and the **SUBJECT ACCOUNT** took place between on or about March 16, 2021 to on or about April 5, 2021. The following is an excerpt from the communications between john.drew87 and the **SUBJECT ACCOUNT**:

john.drew87: You have any young friends? Or sisters?

Grace.\_law then sent one image of a clothed white female. Your affiant then noted the following conversation ensued:

John.drew87: Who's that? And how old is she?

Grace.\_law: 16

John.drew87: How you know her? She's hot as fuck. She can bounce your [her] underage ass all over my cock.

Grace.\_law: Mmm

John.drew87: Would she let me? I'm 23.

Grace.\_law: Yea.

John.drew87: I widh you had younger. I have zero limits.

Grace.\_law: Hehe have u [you] got any younger.

John.drew87: Yeah I got way way younger.

Grace.\_law: Can I see

John.drew87: What's they youngest you wanna see?

Grace.\_law: As young [as] u [you] got

John.drew87: Clothes or nude

Grace.\_law: Both

John.drew87 then sent **SUBJECT ACCOUNT** a total of four images depicting the following:



1. One image depicting a prepubescent female, white with blond hair wearing multi-colored tight fitting spandex shorts and a black sports bra. The female is posed with her buttocks facing the camera and she is looking back over her shoulder.
2. One image depicting a prepubescent female, white with blond hair wearing a pink shirt, brown tights, and blue jean shorts which had been cut in a manner as to display the minor female's buttocks. The female in the image is kneeling on the floor of a bathroom. The female is posed in a manner where buttocks facing the camera.
3. One image depicting a naked prepubescent female, white posing in front of a mirror with her hands behind her head.
4. One image depicting a prepubescent female, white with black hair wearing a white shirt and white thong underwear. In the image the female is lying on her stomach with her legs spread on the tile floor of a bathroom. The female is looking back over her shoulder.

In response to the four images sent by John.drew87, the following comments were noted by your affiant:

Grace.\_law: Mmmmm.

John.drew87: Whatcha think?

Grace.\_law: Hot af [as fuck]. More.

John.drew87: Show me some stuff first.

Your affiant observed that Grace.\_law then sent two images depicting the same, nude pubescent female. In the first image, the minor female is exposing her nude breasts. In the second image, the minor female is fully nude and exposing her breasts and pubic area to the camera. After John.drew87 received the images from the **SUBJECT ACCOUNT**, your affiant then noted the following conversation occurred:

John.drew87: Who's she?

Grace.\_law: Charli

John.drew87: How old is she and how do you know her?

Grace.\_law: 16 tiktok

John.drew87: She know you are sending me these?

Grace.\_law: Yeaa

John.drew87 then sent Grace.\_law the following nine images:

1. One image depicting a prepubescent female, white wearing a multi-colored shirt which was pulled up to expose her nude breasts.
2. One image depicting a mature female, white and a prepubescent female, white. The prepubescent female is observed to be sticking out her tongue which has a whiteish substance on it similar to semen as noted by your affiant.
3. One image depicting a prepubescent female, white wearing a two piece lavender swimming suit at an indoor swimming pool.
4. One image depicting a female, white with dark hair of undetermined age wearing pink underwear and bra. In the image the female is bent over a bed with a pink sheet. The female is looking back at the camera.
5. One image of depicting two nude prepubescent females lying on their backs with their breasts exposed. One of the minor females appears to have a whiteish substance on her stomach similar to semen as noted by your affiant.
6. One image depicting a pubescent female wearing a white coat over a black bra and panties.
7. One image depicting a pubescent female, white posing naked with her breasts exposed.
8. One image depicting a prepubescent female, white wearing white bra and translucent white underwear.
9. One image depicting a prepubescent female, white with blonde hair wearing white underwear and with her nude breasts exposed

In response to receiving the images, **SUBJECT ACCOUNT** asked “any around 14” and in response, John.drew87 wrote “Yeah why?” After this message the conversation terminated.

47. Preservation letters were served to Kik Messenger for the Kik username Grace.\_law on or about June 15, 2021 and again on or about August 11, 2021.

48. On or about July 7, 2021, an administrative subpoena was served on Kik requesting subscriber information for Kik username Grace.\_law. On or about August 3, 2021, Kik responded to that subpoena with the following information:

Email Address:	glaw3344@gmail.com
Registration Date:	February 25, 2021
User Location	Europe/London

49. In addition, Kik provided a list of IP addresses that were used to access the Kik account for Grace.\_law. A subsequent review of the IP address log provided indicated that the following IP addresses were used to access the Grace.\_law Kik account.

- a. 82.27.158.253
- b. 86.0.4.17
- c. 212.219.8.107
- d. 82.132.213.24
- e. 212.219.8.105
- f. 2.24.203.245

50. An analysis of the IP addresses provided in the Kik subpoena response indicated that the service providers for those IP addresses were all located in the United Kingdom.

51. On or about August 25, 2021, a preservation letter and administrative subpoena were served on Google for the Gmail account glaw3344@gmail.com. The results of the administrative subpoena are still pending.

## **VI. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN MINORS.**

52. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved receiving, distributing, and/or collecting child pornography:

- a. Those who exchange and/or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.
- b. Those who trade and/or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials



for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Those who trade and/or collect child pornography sometimes maintain hard copies of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- d. Those who trade and/or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and have been known to maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- e. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

53. Based upon the conversations between user of the Kik account username John.drew87 and the unknown individual utilizing **SUBJECT ACCOUNT**, and the facts learned during the investigation in this case, namely, that MERRY admitting to requesting and possessing child pornography on Twitter and Kik, your affiant has reason to believe that MERRY has a sexual interest in minors and has viewed, sought out, received, or distributed visual depictions of minors engaged in sexually explicit conduct. Your affiant therefore submits



that there is probable cause to believe the evidence of the offenses of receipt, distribution, and possession of child pornography will be located on the **SUBJECT ACCOUNT** which communicated with MERRY about the exchange of images of child sexual abuse material.

## **VII. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

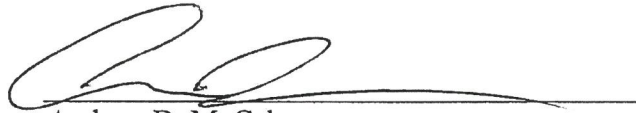
54. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.

## **VIII. CONCLUSION**

55. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2252 and 2252(a) – distribution, transmission, receipt, and/or possession of child pornography, have been committed, and evidence of those violations is located on the **SUBJECT ACCOUNT**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNT** described in Attachment A, and the seizure of the items described in Attachment B.

56. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on MediaLab, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

57. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that has jurisdiction over the offense being investigated." 18 U.S.C. § 271 I (3)(A)(i).



Andrew D. McCabe  
Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me this 18th day of September 2021.



Elizabeth A. Preston Deavers  
United States Magistrate Judge  
United States District Court, Southern District of Ohio



**ATTACHMENT A**

**DESCRIPTION OF PROPERTY TO BE SEARCHED**

This warrant applies to information, including the content of communications, associated with the following Kik account:

- **Kik username Grace.\_law**

which is stored at the premises owned, maintained, controlled, or operated by MediaLab, Inc. located at 1237 7<sup>th</sup> St., Santa Monica, CA 90401.



**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

**I. Information to be disclosed by MediaLab, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab, Inc. is required to disclose the following information to the government for the **SUBJECT ACCOUNT** listed in Attachment A:

- (a) All basic subscriber information including:
  - a. Kik username
  - b. Email address
  - c. Phone number
  - d. Display name
  - e. Kik account creation date and IP address
  - f. Timestamp and IP address of account logins and logouts
- (b) All photos or videos taken using the Kik app's camera, and/or shared with the user's friends, or in a group chat or individual chat, including metadata associated with such images or videos.
- (c) All messages sent from the account identified in Attachment A to any other Kik users.
- (d) All text and multimedia messages stored and presently contained in, or on behalf of the account or identifier;
- (e) All Kik chat groups in which the identified account is a member.
- (f) A complete list of the identified account's contact list and chat partners deleted and undeleted.
- (g) All user typed messages, audio notes, and video notes to friends within the Kik app using the chat feature.
- (h) All opened and unopened one-to-one chats, to include chats sent in groups.
- (i) All user saved messages.
- (j) All device-level location services maintained by Kik.
- (k) All activity logs for the account and all other documents showing the user's posts, chats, and other activities on Kik;
- (l) All other records of communications and messages made or received by the user.

- (m) All IP logs, including all records of the IP addresses that logged into the account;
- (n) All past and present contacts created by the identified user engaging in chats with another Kik user;
- (o) All records of Kik searches performed by the account;
- (p) The types of service utilized by the user;
- (q) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (r) All privacy settings and other account settings, including privacy settings for individual Kik posts and activities, and all records showing which Kik users have been blocked by the account;
- (s) All records pertaining to communications between Kik and any person regarding the user or the user's Kik account, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252 and 2252(a) – distribution, transmission, receipt, and/or possession of child pornography, involving the accounts of the user with Kik username identified in Attachment A, information pertaining to the following matters:

- (a) Evidence indicating how and when the Kik account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Kik account owner;
- (b) Evidence indicating the Kik account owner's state of mind as it relates to the crime under investigation; pertaining to the production, possession, receipt, coercion, enticement or distribution of child pornography and child erotica.
- (c) Evidence of communications related to the possession, receipt, or distribution of child pornography and/or, the coercion or enticement/attempted coercion or enticement of a minor to engage in illegal sexual activity.
- (d) Evidence the user possessed, exchanged or requested visual depictions of minors, from other adults or minors themselves, whether clothed or not, for comparison to any child

pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.